Problem 1 Modular arithmetic & Euler's totient function

1.a Modular arithmetic

Let n be a positive integer. Solve the following exercises.

1) $13 \bmod 5$
2) $-1 \bmod 12$
3) $118 \bmod 5$
4) $-135 \bmod 7$
5) $(6n+1) \bmod 3$
6) $(12n^4 + 9n^2 + 1) \bmod 3$
7) $(5n^2 + 3n - 1) \bmod n$
8) $(113 + 61) \bmod 5$
9) $(182 - 423) \bmod 6$
10) $(7 \cdot 8) \bmod 7$
11) $(30 \cdot 19) \bmod 7$
12) $(6 \cdot 6) \bmod 7$

1.b Euler's totient function

Find the value of Euler's totient function:

1) $\varphi(10)$
2) $\varphi(41)$
3) $\varphi(42)$
4) $\varphi(2^3 \cdot 7^1)$
5) $\varphi(2^{10})$
6) $\varphi(2^3 \cdot 3^8 \cdot 5^1 \cdot 7^2)$

1.c Magic tricks

Without calculators or computers, solve the following problems. Use number-theoretic properties.

1) Find the last decimal digit of 3^{2023}.
2) Find the value of

$$(1! + 2! + 3! + ... + 2024!) \bmod 8.$$

3) Find the value of

$$(1! \cdot 2! \cdot ... \cdot 2024!) \bmod 8.$$

4) Find the value of

$$2023^{2025} \bmod 2024.$$

5) Find the value of

$$2023^{2022^{2021}} \bmod 5.$$

6) Find the value of

$$2^{2^{2^{2^{2^{2}}}}} \bmod 65537.$$

Be careful: $a^{(b^c)} \neq (a^b)^c$.
You may find it also useful that 65537 is not a random number here.

7) Find the value of $f(76) \bmod 11$, where $f(x) = x^{10} + 4x^7 - 22x^4 + 101$.

Problem 2 Euclidean Algorithm & Extended Euclidean Algorithm

2.a Euclidean Algorithm

The function gcd means the greatest common divisor.

Find the value of the following expressions without resorting to exhaustive search or the method of the Sieve of Eratosthenes.

1) $\gcd(67, 14)$

2) $\gcd(-67, 14)$

3) $\gcd(261, 233)$

4) $\gcd(225, 0)$

5) $\gcd(999\,999, 1\,000\,000)$

6) $\gcd(n, n)$, for $n \in \mathbb{Z}$

7) $\gcd(n, n + 1)$, for $n \in \mathbb{Z}$

8) $\gcd(35\,452, 30\,952)$

9) $\gcd(2^2 \cdot 7^{21} \cdot 11^2 \cdot 23^{10},\quad 3^4 \cdot 5^{25} \cdot 7^3 \cdot 11^{18})$

10) $\gcd(7524, 6120, 4626, 1395)$

2.b Extended Euclidean Algorithm

Solve the exercises.

The expression $a^{-1} \bmod n$ means a multiplicative inverse to a modulo n.

1) $x = 3^{-1} \bmod 14$

2) $261x + 233y = \gcd(a, b)$

3) $261x \equiv 11 \pmod{233}$

4) $x = 261^{-1} \bmod 233$

5) $119x + 567y = \gcd(a, b)$

6) $119x \equiv 35 \pmod{567}$

7) $x = 119^{-1} \bmod 567$

8) $x = (n - 1)^{-1} \bmod n$, where n is an integer greater than 1.

Problem 3 Chinese Remainder Theorem

Find x for the following systems of congruences:

$$1)\begin{cases} x \equiv 151 \pmod{255} \\ x \equiv 113 \pmod{172} \end{cases}$$

$$2)\begin{cases} x \equiv 16 \pmod{13} \\ x \equiv 13 \pmod{37} \\ x \equiv 11 \pmod{23} \end{cases}$$

$$3)\begin{cases} x \equiv 3 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{5} \\ x \equiv 7 \pmod{11} \end{cases}$$

Problem 4 Fast Exponentiation

4.a Square-and-Multiply

In order to find the value of $a^b \bmod n$ we can multiply a by itself b times. But it is slow, and there are much faster techniques.

Use Square-and-Multiply algorithm to find:

$$13^{147} \bmod 250.$$

4.b Exponentiation using CRT

If we know the canonical form of the modulus, we can accelerate the calculation of $a^b \bmod n$ with Chinese remainder theorem. Find:

$$3^{4468} \bmod 5681, \quad \text{where } 5681 = 13 \cdot 19 \cdot 23.$$

Note that if $N \vdots n_i$, then $(a \bmod N) \bmod n_i = a \bmod n_i$.

PROBLEM 5 Breaking RSA

Alice needed to send her m credit card number to the Bank using secure RSA encryption. To encrypt m, she used the Bank's public RSA key: (e, N). At the output of the encryption function, she received the ciphertext c, which she then sent to the bank. We eavesdropped their communication and received c. We also used some advanced algorithm to find the factorization of the number N.

Break this RSA instance, then find m to get access to her money. You may use computer, but it is forbidden to do exhaustive search (a.k.a. brute force). All the methods that are practiced in other tasks of homework #1 are sufficient to break it. Check Materials section for RSA description.

Here is all information we could get:

- Bank's public key (e, N):

$$e = 251$$

$$N = 27029 = 179 \cdot 151$$

- Alice's ciphertext c:

$$c = 23947$$